计算机科学
COMPUTER SCIENCE

基于融合序列的远控木马流量检测模型

吴丰源, 刘明, 尹小康, 蔡瑞杰, 刘胜利

引用本文

吴丰源, 刘明, 尹小康, 蔡瑞杰, 刘胜利. 基于融合序列的远控木马流量检测模型[J]. 计算机科学, 2024, 51(6): 434-442.

WU Fengyuan, LIU Ming, YIN Xiaokang, CAI Ruijie, LIU Shengli. Remote Access Trojan Traffic Detection Based on Fusion Sequences [J]. Computer Science, 2024, 51(6): 434-442.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230400159

基于融合序列的远控木马流量检测模型

吴丰源[1,2]　刘　明[2]　尹小康[2]　蔡瑞杰[2]　刘胜利[2]
1 郑州大学网络空间安全学院　郑州 450001
2 信息工程大学网络空间安全学院　郑州 450001
(lingtree@qq.com)

摘　要　针对现有远控木马流量检测方法泛化能力较弱、表征能力有限和预警滞后等问题,提出了一种基于融合序列的远控木马流量检测模型。通过深入分析正常应用网络流量与远控木马流量在包长序列、包负载长度序列和包时间间隔序列方面的差异,将流量表征为融合序列。将融合序列输入 Transformer 模型,利用多头注意力机制与残差连接挖掘融合序列内在联系,学习木马通信行为模式,有效地提升了对远控木马流量的检测能力与模型的泛化能力。所提模型仅需提取网络会话的前 20 个数据包进行检测,就能够在木马入侵早期做出及时预警。对比实验结果表明,模型不仅在已知数据中具有优异的检测效果,在未知流量测试集上同样表现出色,相比当前已有的深度学习模型,各项检测指标有较大提升,在远控木马流量检测领域具备实际应用价值。

关键词:远控型木马检测;融合序列;Transformer 模型;多头注意力机制;木马行为模式
中图分类号　TP393.08

Remote Access Trojan Traffic Detection Based on Fusion Sequences

WU Fengyuan[1,2],LIU Ming[2],YIN Xiaokang[2],CAI Ruijie[2] and LIU Shengli[2]
1 School of Cyber Science and Engineering,Zhengzhou University,Zhengzhou 450001,China
2 School of Cyberspace Security,Information Engineering University,Zhengzhou 450001,China

Abstract　In response to the issues of weak generalization ability,limited representation capability,and delayed warning in existing remote access Trojan(RAT) traffic detection methods,a RAT traffic detection model based on a fusion sequence is proposed. By deeply analyzing the differences between normal network traffic and RAT traffic in packet length sequence,packet payload length sequence,and packet time interval sequence,traffic is represented as a fusion sequence. The fusion sequences are input into a Transformer model that utilizes multi-head attention mechanisms and residual connections to mine the intrinsic relationships within the fusion sequences and learn the patterns of RAT communication behavior,effectively enhancing the detection capability and generalization ability of the model for RAT traffic. The model only needs to extract the first 20 data packets of a network session for detection and can issue timely warnings in the early stages of Trojan intrusion. Comparative experimental results show that the model not only achieves excellent results in known data but also performs well in unknown traffic test sets. Compared with existing deep learning models,it presents superior performance indicators and has practical application value in the field of RAT traffic detection.

Keywords　Remote access Trojan detection,Fusion sequences,Transformer model,Multi-head attention mechanism,Trojan behavior patterns

1　引言

网络安全一直是当前社会发展中不可忽视的问题。随着互联网技术的飞速进步,各种恶意攻击变得更加复杂,防范难度也不断增大。木马病毒作为最常见的一种恶意软件,具有极大的危害性,这类病毒不仅可以窃取用户的个人信息和敏感数据,甚至可以控制被感染设备,带来了极大的经济损失和安全风险[1]。远程控制木马(Remote Access Trojan,RAT)(下文称"远控木马")则是木马病毒中一种危害性极高的类型,它通过不正当手段获得主机管理员权限,并能够通过网络操控用户主机。根据中国互联网安全协会的数据显示,远控木马攻击病毒在我国网络安全攻击事件中所占比例高达

到稿日期:2023-04-24　返修日期:2023-07-24
基金项目:国家重点研发计划(2019QY1300);科技委基础加强项目(2019-JCJQ-ZD-113)
This work was supported by the National Key R&D Program of China(2019QY1300) and Science & Technology Commission Foundation Strengthening Project(2019-JCJQ-ZD113).
通信作者:刘胜利(mr_shengliliu@163.com)

57.4%[2]，远超过其他类型的恶意软件，同时其攻击手法不断演进，危害性和隐蔽性得到增强。

当前针对远控木马流量检测的技术主要分为3类：1）基于特征的木马检测方法；2）基于行为的木马检测方法；3）基于机器学习的木马检测方法。基于特征的木马检测方法提取待流量中的某些特征（如端口号[3]）来匹配病毒库信息以检测木马，但随着病毒种类增多与加密技术的广泛应用[4]，这种检测方法性能下降明显。基于行为的木马检测方法关注流量的行为和模式，相比基于特征的方法具有更强的泛化能力[5]，但前期需要分析大量的数据且仍受到数据加密的影响。传统的机器学习方法的有效性主要依赖人工设计的特征，如协议特征、进程特征和统计特征等[6]，以及SVM，XGBoost和k-means等分类算法，虽取得了较好的检测效果，但仍存在泛化能力较弱、对木马行为模式挖掘能力较弱等问题。

深度学习的出现打破了传统机器学习方法中需要人工设计和选择特征的局限性。然而，如何将流量表征为合适的形式输入到深度学习模型成为关键问题。将流量表征为图像的方式简单直接且能够尽可能地保留原始流量数据，但容易丢失时序信息且数据的维度较高；将流量表征为时间序列可以捕捉到数据的动态变化特征，但可能会忽略数据的空间结构。将流量表征为拓扑图可以很好地表示流量数据之间的关联性，但其数据结构过于复杂。

综上所述，当前远控木马流量检测方法往往存在泛化能力弱、表征能力有限以及对木马入侵预警不及时等问题。为应对上述挑战，本文从远控木马行为模式、木马隐藏自身需要、人与机器行为差异等多个角度，提出了一种基于融合序列的远控型木马检测模型。本文的主要贡献如下。

1）提出了一种将流量表征为融合序列的方法。该方法通过将包长、包负载长度和包时间间隔组合成融合序列，捕捉流量数据中的时序关系，挖掘潜在联系并捕捉木马流量在不同维度上的异常和规律，在保证数据完整与减少资源开销的同时，实现更为精确的流量表征。

2）将融合特征序列与Transformer模型相结合，利用多头注意力机制学习融合序列多个维度间的复杂关系，挖掘木马行为模式以增强模型泛化能力。此外，通过残差连接和层归一化，解决了梯度消失和梯度爆炸问题，提高了模型训练的稳定性和收敛速度，从而进一步提高了模型的检测准确率。

3）通过对比实验，验证了基于融合序列的木马流量检测模型相比其他方法具有更高的准确率和更强的泛化性能。实验结果证明，在仅收集通信双方前20个数据包的情况下，该模型能够在木马入侵早期及时响应并发出预警，有助于有效防范安全隐患，从而保护网络安全。

2 相关工作

随着研究的深入，国内外学者对远控木马流量的3种检测技术进行了更为深入的探索。

基于特征的木马检测方法[7-9]主要是通过分析木马病毒的特征，如代码特征、网络特征等，对木马流量进行检测。该方法的优点是检测速度快，准确率较高。然而，随着木马病毒的变种和加密技术的发展，特征检测方法面临着很大的挑战。

基于行为的检测方法[10-12]主要是通过分析木马病毒执行时的行为，如系统调用、网络行为等，对木马流量进行检测。由于远控木马的恶意行为具有普遍性，该方法可以有效识别变种木马病毒，具有较强的鲁棒性。然而，行为检测方法的实时性和准确率仍有待提高。Wang等[12]以通信双方交互的第一条TCP流为分析对象，针对上线包及其后续数个数据包，提取包负载大小等序列，把序列中对应数值乘以位置权重求和的方式将流量行为映射为一个特征，最终采用机器学习算法完成检测。这种方法考虑了木马的行为，但是未能挖掘流量序列之间的联系。

随着机器学习和深度学习技术在木马流量检测领域的广泛应用，研究人员通过将特征工程和机器学习算法相结合开辟了新的流量分类领域。然而，这种方法过于依赖专家经验，分类准确率很大程度上依赖于选取的流量特征。Arash等[13]经过长时间的观察与分析，总结了流量的80余种特征，并设计了一款可自动提取流量特征的工具，被广泛用于当前的机器学习方法。Ren等[14]通过计算特征间的皮尔逊相关系数来判断特征的强弱关系，以确定最优阈值，从而进行特征选择。Zou等[15]使用隐马尔可夫模型匹配流量的关键基因子序列，利用SVM等模型实现加密恶意流量的检测。

深度学习则通过端到端的方法，训练大量的木马病毒样本，自动提取有效的特征和行为规律，从而提高检测的准确率和实时性。Wang等[16]将原始流量的字节流数据表征为28 * 28的灰度图像，通过卷积神经网络（Convolutional Neural Network，CNN）对灰度图进行分类的方式区分正常流量与恶意流量。但是，这种方法仅考虑了部分流量信息且泛化能力稍弱。Gu等[17]将虚拟对抗训练模型与半监督深度学习模型mean teacher相结合，提高了模型检测的泛化能力。Li等[18]将流量的字节通过词嵌入转换成字符向量序列，设计了一种CNN与RNN结合的方法学习流量的空间与时间特征，完成对恶意TLS流量的快速识别。Wang等[19]在Li等[18]的基础上将一维多尺度卷积与长短期记忆网络结合，提升了模型的表征能力与泛化能力。文献[20-24]利用图神经网络捕捉网络流量在非欧空间中的复杂拓扑关系，从而提高流量分类的准确性和泛化能力。

虽然深度学习方法省去了繁琐的人工提取特征过程，但是不同的流量表征形式和多样的深度学习模型结构影响了检测的性能、效率与泛化能力。因此，如何选取合适的流量表征形式与设计深度学习模型来提高木马流量检测的准确率和效率，成为了研究的关键问题。

Transformer[25]模型最初是为自然语言处理任务设计的，由于其优异的性能和并行计算能力，近年来已被广泛应用于各种领域。Transformer模型通过自注意力机制来捕捉序列中的长距离依赖关系，能够更好地理解和表示远离彼此的元素之间的关系。在处理融合序列时，这种机制可以有效地捕捉行和列之间的相关性。相比循环神经网络（RNN）和长短时记忆网络（LSTM），Transformer模型在计算时可以实现更高的并行度，加速计算过程。同时，它具有很好的扩展性与灵活性，通过堆叠多个编码器与解码器来增加模型的深度，从而改善模型在处理复杂数字和复杂结构的融合序列时的表现。

Yang 等[26]通过将类别再平衡自训练算法与视觉 Transformer 相结合，实现了在不平衡数据集上识别异常网络流量。

本文方法将流量表征为由包长、包负载长度、包时间间隔所组成的融合序列。这样的表征形式不仅能够准确地保留原始流量的关键数据，还能够在保证时间效率的同时捕捉并利用流量的动态变化，从而为识别和预测木马攻击行为提供有效信息。为了进一步挖掘融合序列中的潜在模式和关系，我们采用了 Transformer 模型。与现有木马流量检测模型相比，Transformer 模型利用多头注意力机制捕捉融合序列间的长距离依赖关系，有助于学习木马行为模式，同时 Transformer 模型利用残差连接和层归一化等设计有效解决了梯度消失和梯度爆炸等问题。这一创新方法旨在解决现有方法在泛化能力较弱、表征能力有限以及预警滞后等方面的问题，提升了对远控木马流量的检测准确性和实时性。实验结果证实了所提模型在未知流量测试集上具有出色的性能，展示了其在远控木马流量检测领域的实际应用价值。

3 基于融合序列的远控木马流量检测模型

远程控制木马通信可以分为建立连接、交互连接和保持连接 3 个阶段[27]。如图 1 所示，在建立连接阶段，为规避防火墙的拦截，现有流行木马常常采用反弹式连接方式，此时服务端通过 DNS 请求解析动态 IP 并建立连接。在交互连接阶段，控制端主动发送命令，而服务端则提供执行结果，此时包长序列和包负载长度序列往往体现为一个下行小包和数个上行大包的周期循环。在保持连接阶段，服务端和控制端互发心跳包来保持连接不被断开，导致小数据包占比增加。对这些行为的分析有助于识别和检测远程控制木马的攻击行为。

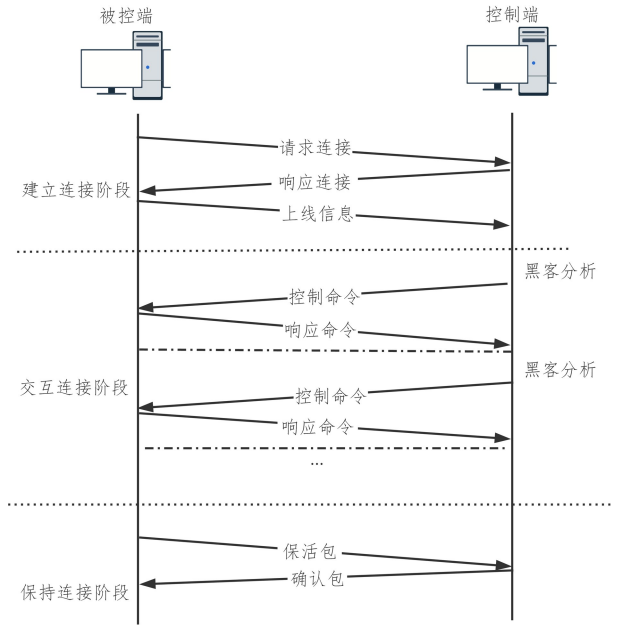


图 1 远控木马通信的 3 个阶段

Fig. 1 Three stages of RAT communication

3.1 融合序列表征

网络流量往往存储为 PCAP 文件格式，它由头部和若干个数据包组成。网络流量数据包是计算机网络中用于在网络层传输数据的基本单位。数据包在网络中传输时，它们包含了源地址、目的地址、负载数据(即所要传输的信息)和控制信息，数据包由头部、负载和尾部组成。其中，头部(Header)的信息用于数据包在网络中正确地传输和路由，它包含了一些关于数据包的元数据，如源地址、目的地址、协议类型等。负载(Payload)是数据包中实际要传输的数据，它可以是任何类型的信息，如文本、图像、音频等。尾部(Tailer)的主要作用是确保数据包在传输过程中没有发生错误或损坏，通常包含了一些校验和错误检测信息，如循环冗余校验(CRC)等。

在网络流量分析中，数据包长、包负载长度以及两个数据包到达的时间间隔是描述网络数据包特征的关键属性。包长序列指单个网络会话中多个数据包的总长度组成的序列；包负载长度序列则由数据包的负载部分长度组成；包时间间隔序列指网络中连续两个数据包之间到达的时间间隔的序列。

如表 1 所列，本文选取了 10 款典型的远控木马和 10 款常用的应用程序进行对比分析。我们对这些应用程序的网络流量进行了深入研究，着重于包长序列、包负载长度序列和包时间间隔序列等方面。研究这 3 个序列有助于挖掘网络流量的行为模式，以便更好地了解正常网络流量与远控木马流量之间的差异。我们将发现的差异总结为以下 4 个方面。

表 1 10 款远控木马与 10 款正常网络应用

Table 1 10 Remote access Trojans and 10 normal network applications

远控木马	正常应用
Ghost, Zeus, fasftuby, dridex, trickbot, NjRAT, flu, nuclearrat, 任我行远控, 上兴远控	Youtube, email, facebook, skype, vimeo, bilibili, LOL, tiktok, 今日头条, 网易云音乐

1)包长序列差异

正常网络流量的包长序列通常呈现出较高的多样性。正常网络应用程序在传输数据时，包长有很大差异。如图 2、图 3 所示，LOL 应用流量的包长最大可达 2 834 字节，而 vimeo 应用流量的包长则是在 0～7 000 内波动，其余的几款应用流量包长虽然受 MTU(以太网最大长度单元)的限制，但仍呈现出多样性。然而，远控木马流量的包长序列会表现出较为集中的特点，这是因为攻击者在发送控制命令或数据包时，通常会使用特定的协议或模式，以便更好地隐藏恶意行为。如图 3 所示，Ghost, NjRAT 等远控木马的典型特征是在小包后出现一个或数个大包的波动。这种模式与远控木马命令交互阶段相符，即黑客发出控制命令后，服务端进行响应。同时，相比正常网络流量，远控木马流量的包长度序列波动更为剧烈，因为攻击者在发送控制命令时，可能会在较短时间内发送多个不同大小的数据包，以完成攻击任务。

2)包负载长度序列差异

正常网络流量的包负载长度序列通常包含各种不同大小的数据包，以满足各种应用程序的需求。远控木马流量的包负载长度序列表现出一定程度的集中性，尤其是在攻击者发送控制命令或少量数据包时。攻击者为了隐藏自己的行为，往往会减少附加数据的数量，因此远控木马流量中负载长度较小的数据包比正常网络流量中的更为常见。

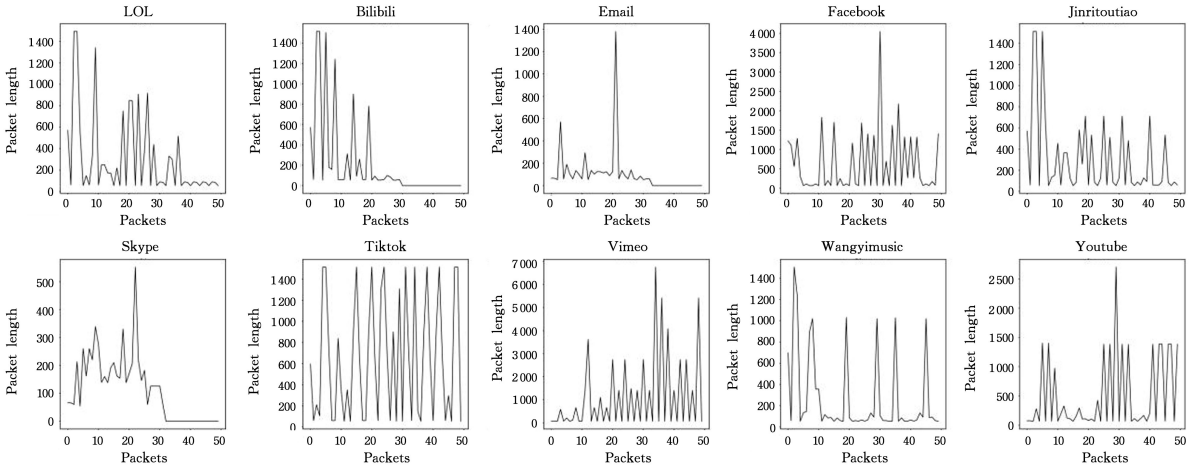


图 2　10 款正常应用流量的包长序列

Fig. 2　Packet length sequence of the traffic of 10 normal applications

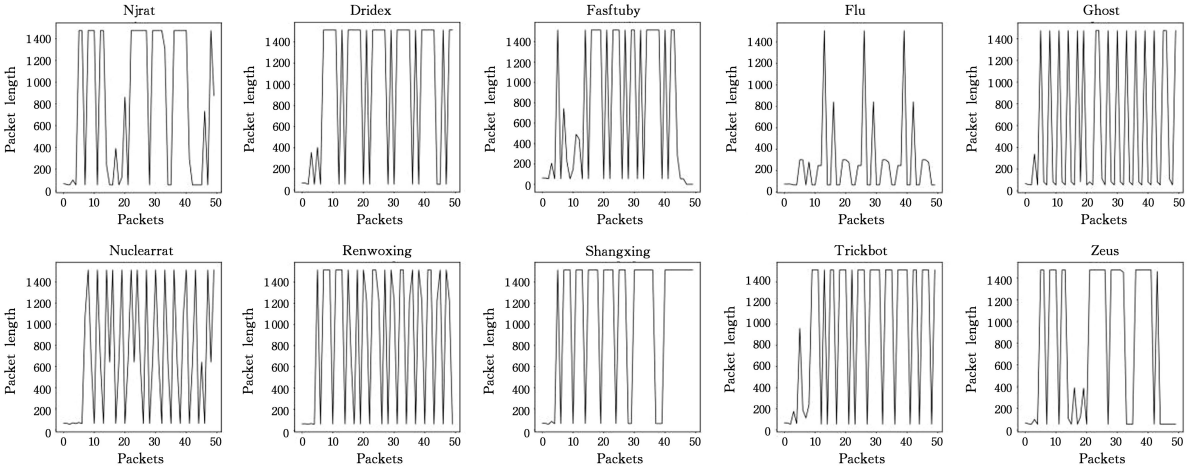


图 3　10 款远控木马流量的包长序列

Fig. 3　Packet length sequence of 10 remote access Trojan traffic

3）包时间间隔序列差异

如图 4、图 5 所示，正常网络流量和远控木马网络流量包时间间隔序列的差异主要体现在时间间隔分布、峰值数量与均值上。在远程控制过程中，攻击者往往需要花费一定时间来处理目标系统的响应，或者为了避免引起注意，故意延长命令和数据包之间的时间间隔，这导致包时间间隔均值高于正常流量。攻击者思考完成进行下一步攻击时，木马流量在包时间间隔序列上表现出了较多的峰值和较高的峰值频率。这意味着在某些特定时刻，木马流量的数据包发送速率会有显著的增加。

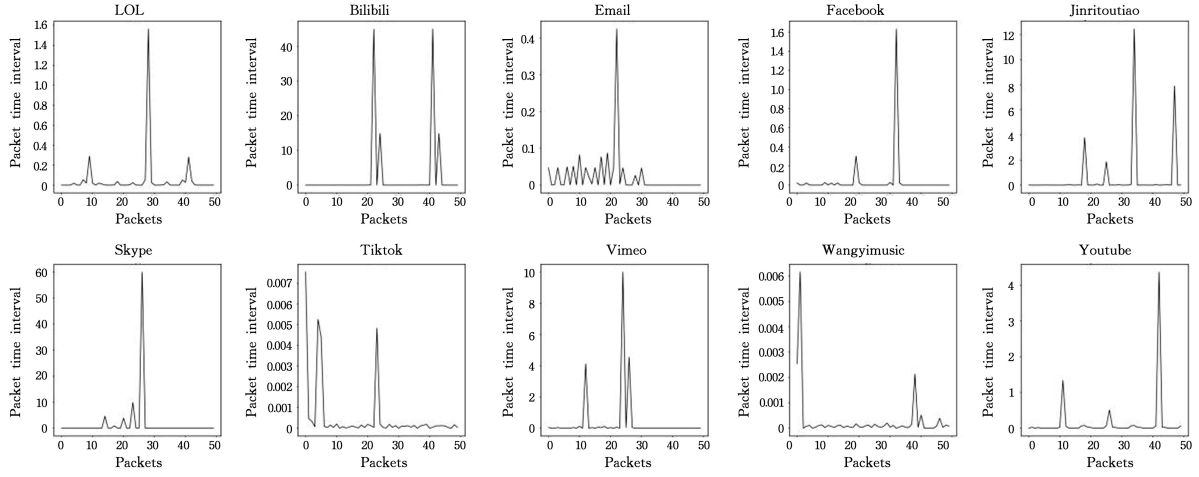


图 4　10 款正常应用流量的包时间间隔序列

Fig. 4　Packet interval sequence of the traffic of 10 normal applications

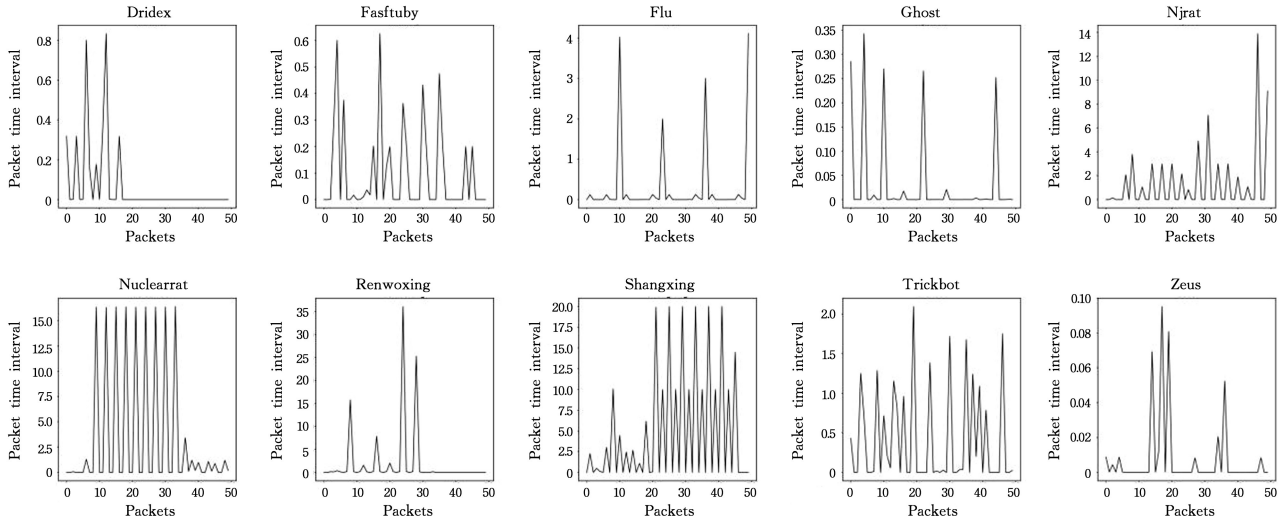


图 5 10 款远控木马流量的包时间间隔序列

Fig. 5 Packet interval sequence of 10 remote access Trojan traffic

4)包长和包负载长度之间的关系差异

在正常网络流量中,包长和包负载长度之间的关系通常呈现出一定的正相关性。例如,当某个应用程序需要发送大量数据时,数据包的包长和包负载长度都较大。然而,在远控木马流量中,包长和包负载长度之间的关系更为复杂,因为攻击者可能会在发送大量控制命令的同时,附加较少的数据,从而使包长和包负载长度之间的关系不明显。

3.2 模型设计

本文模型的架构如图 6 所示。首先对原始流量数据集进行预处理,通过会话切分、序列提取、数据清洗、标记标签等步骤,筛选出需要的数据。通过张量维度调整,将其转换成模型所需的格式,以方便后续的处理。随后,将处理好的数据输入 Transformer 模型中,利用线性层将输入数据映射到高维空间,加入多头自注意力机制使 Transformer 编码器可以捕捉数据中的长距离依赖关系和复杂模型。最后经过多层迭代,将特征向量输入全连接层并映射到目标空间,从而获得模型最终的预测结果。

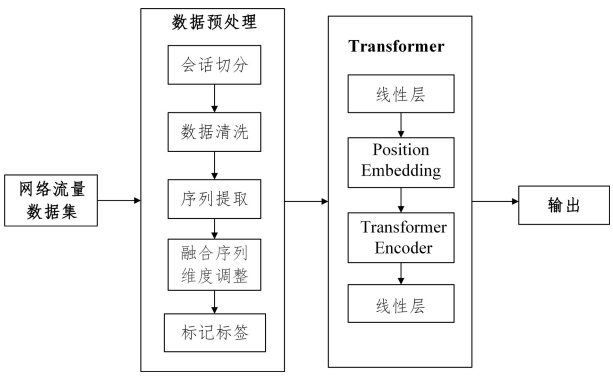


图 6 基于融合序列的 Transformer 模型的整体架构

Fig. 6 Overall architecture of Transformer model based on fusion sequence

3.3 Transformer 模块

本文使用了一个定制化的 Transformer 模型,以更好地处理网络流量序列数据并进行分类。

首先,本文模型接收输入特征序列,尺寸为($batch\_size$, seq_len, $input\_size$),其中 $batch\_size$ 表示批量大小,seq_len 表示序列长度,$input\_size$ 表示输入特征的维度。模型通过以下组件进行处理。

1)嵌入层(Embedding Layer)

输入特征序列首先经过一个线性嵌入层,将输入尺寸从 $input\_size$ 维度转换为 d_model 维度。嵌入层的计算过程可以表示为:

$$E(x)=W_e x+b_e \tag{1}$$

其中,x 表示输入特征,$\boldsymbol{W}_e$和b_e分别表示嵌入层的权重矩阵和偏置项。

2)Transformer 编码器(Transformer Encoder)

嵌入后的特征序列被送入一个由 4 个 Transformer 编码器层组成的 Transformer 编码器。每个编码器层包含一个多头自注意力机制和一个前馈神经网络。编码器层的计算过程可以表示为:

$$\begin{aligned} H^l&=LayerNorm(H^{l-1}+SelfAttention(H^{l-1}))\\ H^l&=LayerNorm(H^l+FFN(H^l)) \end{aligned} \tag{2}$$

其中,H^l表示第 l 层的隐藏状态,LayerNorm 表示层归一化操作,SelfAttention 表示多头自注意力机制,FFN 表示前馈神经网络。

3)全连接层(Fully Connected Layers)

Transformer 编码器的输出经过两个全连接层,将特征从维度映射到最终的分类输出尺寸 output_size。全连接层的计算过程可以表示为:

$$y=W_2\cdot GELU(W_1\cdot H+b_1)+b_2 \tag{3}$$

其中,y 表示分类输出,$\boldsymbol{W}_1$,b_1,$\boldsymbol{W}_2$和b_2分别表示全连接层的权重矩阵和偏置项,$GELU$ 表示激活函数。为了提高模型的泛化能力,本文在全连接层之间添加了层归一化(Layer Normalization)和 dropout 操作。

通过这些处理步骤,本文模型能够在每个会话中捕捉到更为详细的信息,并根据提取的特征进行网络流量分析和分类。我们使用会话作为基本单位,以便在处理过程中保留

通信双方之间的交互信息，从而使模型能够更准确地识别正常流量与木马流量之间的差异。

4 实验与结果分析

本文实验分为 3 个部分。第一部分是模型参数选择实验，通过 24 组调参实验选择最佳的 Transformer 模型参数；第二部分是序列数据包数选择实验，设置 5 组对比实验选择最佳的检测序列长度；第三部分是模型对比实验，将本文方法与其他 4 组文献中的方法分别在已知数据集和未知测试集上做对比实验，验证基于融合序列的木马流量检测模型的有效性与泛用性。

4.1 实验环境及参数设置

实验操作系统为 Windows10 专业版，GPU 型号为 GeForce RTX2070，cuda 版本为 11.7，使用 Anaconda3 编辑环境，python 版本为 3.10。

实验中涉及的参数如下：单次训练样本数 batch_size 为 64，训练轮数 epochs 为 20，模型选择交叉熵作为损失函数，Adam 优化算法，学习率 lr 为 0.0001。

4.2 数据集与数据预处理

在木马流量检测领域，目前尚缺乏权威的公开数据集。为了充分利用现有资源并提高检测效果，本研究在选择模型训练数据集时，综合考虑了多个与木马流量检测相关的公开数据集。具体而言，恶意流量选自捷克技术大学（CTU）研究人员从真实网络环境中收集的 6 款远控木马应用流量[28]，如 NjRAT，Ghost 等，总计 2.1GB，共包含 135724 条会话。而正常流量则来自 UNB CIC-IDS2017 入侵检测数据集[29]，涵盖了 Skype，Facebook 等正常应用流量，总计 9.6 GB，共包含 124589 条会话。我们采用 8∶2 的比例将数据集划分为训练集与测试集，以检测模型的性能表现。

为了验证所构建模型的扩展性和泛化能力，本文单独设置了未训练数据集作为未知测试集。未知测试集中的恶意流量来自实验室收集的 10 款木马软件，如灰鸽子、Evilotus 等，总计 1.67 GB，共包含 2934 条会话。正常流量则选自 UNB ISCX VPN-nonVPN2016 数据集[30]，总计 5.23 GB，共包含 6592 条会话。值得注意的是，在实际网络环境中，木马流量相比正常流量通常更少。为了更贴近实际情况并提高检测模型的实用性，本文在测试集中将木马流量设置得少于正常流量。这种设计有助于验证模型在面对现实网络环境中数据分布不均的情况下的有效性和稳定性。数据集的详细情况如表 2 所列。

表 2 数据集的详细信息

Table 2 Dataset details

数据集类型	数据来源	流量类型	木马/应用名称	数据量/GB	会话数量
数据集	CTU[28]	木马	NjRAT，Ghost 等	2.10	135724
数据集	UNB CIC-IDS2017[29]	正常	Skype，Facebook 等	9.60	124589
未训练数据集	实验室收集	木马	灰鸽子、Evilotus 等	1.67	2934
未训练数据集	UNB ISCX VPN-nonVPN2016[30]	正常	Youtube 等	5.23	6592

在网络流量分析中，原始的网络数据（PCAP 文件）往往需要按照特定的方式进行切分，以便提取有效的信息和特征。目前，主要存在 3 种切分方式，分别是基于包、基于流和基于会话的切分方法。基于包的切分方式将原始 PCAP 文件中的每个数据包单独提取出来，形成独立的数据单元，便于对单个数据包进行分析和处理。这种方式常被应用于网络攻击的深入分析，但其处理效率较低，且会丢失数据包之间的关系信息。基于流的切分方式将 PCAP 文件中具有相同五元组（源 IP 地址、目的 IP 地址、源端口、目的端口、协议）的数据包视为一个流，以此为切分单位。这种方法在提高处理效率的同时，保留了部分数据包之间的关系。基于会话的切分方式将双向流视为切分的基本单位，从而保存通信双方的交互流量以及更多信息，确保了数据之间的完整性。

本文采用基于会话的切分方式对原始 PCAP 文件进行处理，具体过程如下：

1）使用 SplitCap 工具[31]将原始 PCAP 文件切分为不同的会话。

2）会话切分完成后，部分数据会丢失信息，例如一个完整的 TCP 会话应至少包含 3 次握手和数据交互环节。因此，我们需要筛选并删除应用层中没有数据的会话。

3）对于每个会话，我们抽取前 20 个数据包的包长序列、包负载长度序列、包时间间隔序列。若当前会话的数据包数少于 20，则在序列末尾补 0。

4）将每个会话中抽取的 3 个序列的数据维度调整为 20 * 3 的融合序列。

5）根据序列的类别，将相应的序列数据存放在对应标签命名的文件夹下。

通过上述预处理过程，我们移除了冗余和无效数据，获取了会话的融合序列表征，为后续实验作铺垫。通过这种方法，我们能够深挖流量数据的信息，有助于更好地学习木马行为模式，从而提高基于融合序列的木马流量检测模型的实际性能。

4.3 评价指标

为了评价二分类情况下分类器的性能，本文采用了准确率（Accuracy）、召回率（Recall）、F1 值（F1-score）和 AUC 值（Area Under the Curve）等指标。

首先，介绍 4 种预测结果与真实结果的情况。TP（True Positive）表示预测当前流量是木马流量，且实际上是木马恶意流量；FN（False Negative）表示预测当前流量是正常流量，但实际上是木马流量；FP（False Positive）表示预测当前流量是木马流量，但实际上是正常流量；TN（True Negative）表示预测当前流量是正常流量，且实际是正常流量。基于这些情况，我们使用以下二分类木马流量检测的评价指标。

1）准确率（Accuracy）：是分类器正确预测的样本数量占总样本数量的比例，能够衡量分类器在预测正类和负类时的整体性能。

$$Accuracy=\frac{TP+TN}{TP+TN+FP+FN} \tag{4}$$

2)召回率(Recall):指分类器能够正确判定正例样本的能力,计算式为:

$$Recall=\frac{TP}{TP+FN} \tag{5}$$

3)F1 值(F1-score):是精确率和召回率的调和平均值,其计算式为:

$$F1score=\frac{2\cdot TP}{2\cdot TP+TP+FN} \tag{6}$$

4)AUC 值(Area Under the Curve):是 ROC 曲线(Receiver Operating Characteristic Curve)下的面积,反映分类器在不同阈值下的表现。

4.4 实验结果

1) Transformer 模型参数选择

本文探索了 Transformer 模型参数对木马流量检测性能的影响。我们选择了两个关键参数,即 *nhead* 和 *num_layers*,并对其进行了广泛的实验评估。*nhead* 指每个多头注意力机制中的头数,它决定了模型的注意力集中程度和并行计算能力;*num_layers* 指编码器和解码器中的层数,它可以影响模型的深度和表达能力。

我们通过尝试不同的参数组合来比较模型的性能。具体地,我们选择了 nhead 的值为 1,2,4,8,*num_layers* 的值为 1,2,3,4,5,6,共计 24 种参数组合。我们训练了每个模型,并对其进行了测试,以评估其在检测木马流量方面的性能。实验的结果如图 7、图 8 所示,其中 x 轴为 Transformer 模型的编码器和解码器层数 *num_layers*,y 轴为评价指标,图例为多头注意力并行头数 *nhead*。

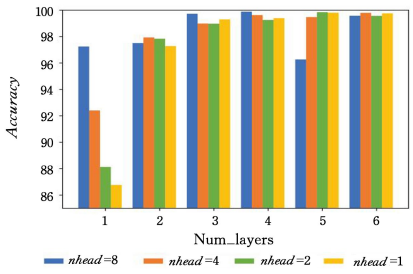


图 7 不同超参数组合的平均准确率实验结果

Fig. 7 Average accuracy experimental results of different combinations of hyperparameters

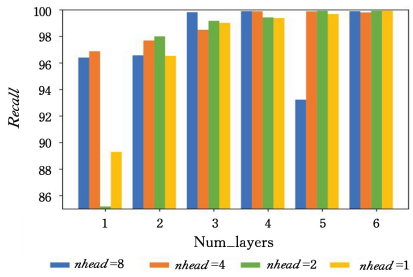


图 8 不同超参数组合的平均 Recall 值实验结果

Fig. 8 Average Recall of different combinations of hyperparameters

本文的实验结果表明,增加编码器层数与注意力头数并不总是能够提升模型的性能。过多的注意力头数会放大噪声的干扰,从而影响模型的性能;而过多的层数增加了模型的复杂度,导致模型过拟合数据。当 *nhead*=8 且 *num_layers*=4 时,模型的准确率与召回率分别为 99.89%和 99.91%,均优于其他组合。因此,本文最终选取编码器层数 *num_layers* 为 4,多头注意力头数 *nhead* 为 8 的 Transformer 模型。

2)会话数据包数选择

本节旨在研究木马流量检测中数据包数量对检测效果的影响。为此,本文采用了 5 组对照实验,分别提取每个会话的前 10,20,30,40,50 个数据包的信息。我们对每个会话进行了分析,并比较了 5 组实验的结果,如图 9 所示。其中,x 轴为数据包的数量,y 轴为评价指标分数。

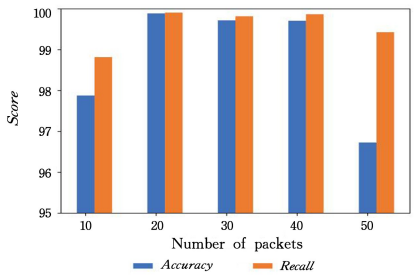


图 9 不同序列长度的平均准确率与召回率实验结果

Fig. 9 Experimental results of average accuracy and recall rate of different sequence lengths

根据实验结果可以发现,在提取前 20 个数据包时,木马流量检测的性能达到了最佳效果。这是因为在前 20 个数据包中,木马至少已经经历建立连接和数次交互的过程,这有助于模型可以更好地捕捉到木马的行为模式。当数据包数量过少时,模型无法充分学习木马的行为特征,而数据包过多时,会放大噪声和数据填充方式的影响,导致检测性能下降。因此,我们选择提取前 20 个数据包作为我们的标准实验流程,并在后续实验中使用该方案。

3)不同方法的对比

为进一步验证融合序列 Transformer 模型的有效性与泛用性,本文选取了 4 种模型(CNN,CNN-LSTM,BiLSTM,Stacking)作为对比模型进行实验。CNN 模型[16]将图像字节流信息转换成灰度图输入卷积神经网络中进行特征提取并分类。CNN-LSTM[32]分别用卷积神经网络与长短时记忆网络来学习流量的空间与时间特征。BiLSTM 模型[33]在输入序列的前项和后向方向上同时进行处理,从而更好地捕捉序列中的信息。文献[34]采用集成学习 Stacking 策略,在第一层采用随机森林、XGBoost、SVM 这 3 种分类器,第二层采用逻辑回归分类器,从流量中提取 64 种特征进行流量分类。我们分别在已知流量数据集和未知流量测试集上进行了实验,实验的结果如表 3 和表 4 所列。

表 3 不同方法在测试集上的性能表现

Table 3 Performance of different methods on test datasets

(%)

模型	*Accuracy*	*Recall*	*F1-Score*	*ROC-AUC*
CNN	99.92	99.92	99.92	99.91
CNN+LSTM	99.96	99.97	99.96	99.96
BiLSTM	98.24	98.09	98.32	99.76
Stacking	98.95	98.96	98.96	98.93
Transformer (本文方法)	99.91	99.91	**99.90**	99.91

表 4 不同方法在未知数据测试集上的性能表现

Table 4 Performance of different methods on unknown datasets

(%)

模型	*Accuracy*	*Recall*	*F1-Score*	*ROC-AUC*
CNN	81.37	85.51	73.88	82.52
CNN+LSTM	81.29	78.77	72.17	80.59
Bilstm	72.11	69.17	63.21	69.17
Stacking	65.34	65.66	67.82	65.19
Transformer（本文方法）	**91.23**	**91.24**	**90.49**	**91.23**

表 3 列出了在已知数据测试集上，各个模型的性能指标。从表中可以看出，CNN，CNN+LSTM，BiLSTM，Stacking 和 Transformer 模型在 Accuracy，Recall，F1-Score 和 ROC-AUC 方面均表现优异。尤其是 CNN+LSTM 模型，其 Accuracy，Recall，F1-Score 和 ROC-AUC 指标分别达到了 99.96%，99.97%，99.96%和 99.96%，在这 5 种模型中表现最佳。然而，Transformer 模型的性能也相当出色，各项指标均超过了 99.9%，说明在已知数据测试集上，我们所提出的基于融合序列的木马流量检测模型具有很强的学习能力，可以准确识别出木马流量。

表 4 列出了在未知数据测试集上，各个模型的性能表现。从表中可以看出，在未知数据测试集上，Transformer 模型的性能表现明显优于其他模型，其 Accuracy，Recall，F1-Score 和 ROC-AUC 分别达到 91.23%，91.24%，90.49%和 91.23%。相比之下，CNN，CNN+LSTM，BiLSTM 和 Stacking 模型在未知数据测试集上的性能相对较差。

实验结果显示，在不同的测试集上，各个模型的性能指标存在差异。在已知数据测试集上，各个模型均表现优异，在保持模型稳定的同时能准确识别出木马流量。然而，在未知数据测试集上，Transformer 模型的性能表现明显优于其他模型，其优势在于能够更好地捕捉木马攻击行为模式，提高对未知木马流量的检测准确性。这主要得益于 Transformer 模型的自注意力机制，它能够对输入序列中的每个元素赋予不同的权重，从而更好地挖掘序列中的潜在关系。此外，Transformer 模型还采用了多头注意力机制，可以捕捉不同层次和抽象程度的信息，提高模型的表示能力。另一方面，实验结果也表明，传统的 CNN，CNN+LSTM 和 BiLSTM 等深度学习模型在未知数据测试集上的性能较差，这主要是因为这些模型在处理序列数据时，可能难以捕捉长距离的依赖关系。Stacking 模型在未知数据测试集上的性能弱于上述 3 种深度学习模型，这是由于其依赖于手工提取的特征，可能无法充分捕捉数据中的潜在信息，导致其性能不如 Transformer 模型。

结束语 本文提出了一种基于融合序列的远控木马流量检测方法，用于检测网络通信中可能存在的木马流量，通过学习木马攻击行为和挖掘融合序列中的内在联系，该方法能够有效地完成木马流量检测。该方法提取了网络会话通信的前 20 个数据包的包长序列、包负载长度序列和包时间间隔序列组成的融合序列，并将其输入 Transformer 模型进行训练。实验结果表明，该方法不仅在已知数据集上二分类表现优异，在未训练过的流量集上仍能取得良好的成绩，识别准确率较现有方法高出 10 个百分点，该方法具有较强的泛化能力和较好的应用前景。在现实网络环境中，正常流量要远多于木马流量，在未来的工作中，我们将进一步探索小样本学习方法，以提高模型的鲁棒性和泛化能力。

参 考 文 献

[1] CHEN T，XIANG Y，YANG L，et al. Malware detection using deep neural network on big data platforms[J]. Future Generation Computer Systems，2021，76，291-300.

[2] 2019 China Internet Security Report[R]. Beijing：China Posts and Telecommunications Press，2019.

[3] WANG P H，ZHENG Q H，NIU G L，et al. Port scan detection algorithms based on statistical traffic features[J]. Journal on Communications，2007，28(12)：14-19.

[4] CHEN Z H，CHENG G，XU Z H，et al. A Survey on Internet Encrypted Traffic Detection，Classification and Identification [J]. Chinese Journal of Computers，2023，46(5)：1060-1085.

[5] YU S S，WANG X J，ZHANG Q Q. Detection of Malicious Behavior in Encrypted Traffic Based on Heuristic Search Feature Selection[J]. Computer Science，2022，49(S2)：734-739.

[6] ZHONG F，RAN L. Investigation of Machine Learning Based Network Traffic Classification[C]// 2017 International Symposium on Wireless Communication Systems(ISWCS). Bologna，Italy，2017：1-6.

[7] ALSHAMMARI R，ZINCIR-HEYWOOD A. Investigating two different approaches for encrypted traffic classification[C]// Cybersecurity Applications & Technology Conference for Homeland Security. 2009：83-88.

[8] CABALLERO J，GRIER C，KREIBICH C，et al. Measuring pay-per-install：The commoditizationof malware distribution[C]// The 20th USENIX Conference on Security. 2011：1-15.

[9] BILGE L，DUMITRAS T. Before we knew it：an empirical study of zero-day attacks in the real world[C]// The 2012 ACM Conference on Computer and Communications Security. 2012：833-844.

[10] KASPEREK P，CHORAS M. Behavioral-based detection of RATs using honeypot data[C]// 2014 Federated Conference on Computer Science and Information Systems. 2014：555-561.

[11] ALRABAEE N，SALEEM N，TRAORE I. Detecting remote access trojans：A survey[J]. Journal of Cyber Security and Mobility，2015，4(1)：3-32.

[12] WANG C，GUO C，SHEN G，et al. Research of Remote Access Trojan Early Detection Method Using Sequence Analysis[J]. Journal of Frontiers of Computer Science and Technology，2021，15(12)：2315-2326.

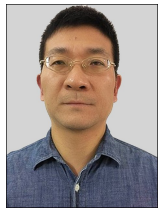
[13] ARASH H L，GERARD D，MOHAMMAD S，et al. Characterization of Tor Traffic Using Time Based Features[C]// 2017 the 3rd International Conference on Information Systems Security and Privacy，Portugal. 2017：253-262.

[14] REN J D，ZHANG Y F，ZHANG B，et al. Classification Method of Industrial Internet Intrusion Detection Based on Feature Selection[J]. Journal of Computer Research and Development，2022，59(5)：1148-1159.

[15] ZOU F T，YU T D，XU W L. Encrypted Malicious Traffic De-

tection Based on Hidden Markov Model[J]. Journal of Software, 2022, 33(7): 2683-2698.
[16] WANG W, ZENG X, YE X, et al. Malware traffic classification using convolutional neural network for representation learning [C]// The 31st InternationalConference on Information Networking(ICOIN 2017). 2017: 712-717.
[17] GU Y H, HUANG B Q, WANG J G, et al. Trojan Traffic Detection Method Based on Semi-Supervised Deep Learning[J]. Journal of Computer Research and Development, 2022, 59(6): 1329-1342.
[18] LI X J, XIE X Y, XU Y, et al. Fast identification method of malicious TLS traffic based on CNN-SIndRNN[J]. Computer Engineering, 2022, 48(4): 148-157, 164.
[19] WANG X T, WANG X, SUN Z X. Network Traffic Anomaly Detection Method Based on Multi-scale Memory Residual Network[J]. Computer Science, 2022, 49(8): 314-322.
[20] SONG Y L, LIU G H, WANG G Z, et al. SDN Traffic Prediction Based on Graph Convolutional Network[J]. Computer Science, 2021, 48(6A): 392-397.
[21] SUN B, YANG W, YAN M, et al. An Encrypted Traffic Classification Method Combining Graph Convolutional Network and Autoencoder[C]// 2020 IEEE 39th International Performance Computing and Communications Conference(IPCCC). Austin, TX, USA, 2020: 1-8.
[22] ZHAO R, DENG X W, WANG Y H, et al. Flow Sequence-Based Anonymity Network Traffic Identification with Residual Graph Convolutional Networks[C]// 2022 IEEE/ACM 30th International Symposium on Quality of Service(IWQoS). Oslo, Norway, 2022: 1-10.
[23] LO W, LAYEGHY S, SARHAN M, et al. E-GraphSAGE: A Graph Neural Networkbased Intrusion Detection System for IoT [C]// 2022 IEEE/IFIP Network Operations and Management Symposium. Budapest, Hungary, 2022: 1-9.
[24] PANG B, FU Y, REN S Y, et al. CGNN: Traffic Classification with Graph Neural Network[J]. arXiv: 2110. 09726.
[25] VASWANIA, SHAZEER N, PARMAR N, et al. Attention is all you need[C]// Advances in Neural Information Processing Systems. 2017: 5998-6008.
[26] YANG Y L, BI Z Z. Network Anomaly Detection Based on Deep Learning[J]. Computer Science, 2021, 48(11): 540-546.
[27] LI W, LI L H, LI J, et al. Characteristics Analysis of Traffic Behavior of Remote Access Trojan in Three Communication Phases[J]. Netinfo Security, 2015(5): 10-15.
[28] GARCÍA S, GRILL M, STIBOREK J, et al. An empirical comparison of botnet detection methods[J]. Computers & Security, 2014, 45(5): 100-123.
[29] IMAN S, ARASH H L, ALI A G. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization[C]// 4th International Conference on Information Systems Security and Privacy(ICISSP). Portugal, 2018: 108-116.
[30] GERARD D G, ARASH H L, MOHAMMAD M, et al. Characterization of Encrypted and VPN Traffic Using Time-Related Features[C]// The 2nd International Conference on Information Systems Security and Privacy. Italy, 2016: 407-414.
[31] NETRESE C. SplitCap[EB/OL]. [2022-04-20]. https://www.netresrc.com/? page=SplitCap.
[32] ZOU Z, GE J, ZHENG H, et al. Encrypted Traffic Classification with a Convolutional Long Short-Term Memory Neural Network[C]// 20th International Conference on High Performance Computing and Communications. Exeter, UK, 2018: 329-334.
[33] LOTFOLLAHI M, JAFARI S, SHIRALI H, et al. Deep packet: a novel approach for encrypted traffic classification using deep learning[J]. Soft Computing, 2020, 24(3): 1999-2012.
[34] HUO Y H, ZHAO F Q. Analysis of Encrypted Malicious Traffic Detection Based on Stacking and Multi-feature Fusion[J/OL]. Computer Engineering. https://doi.org/10.19678/j.issn.1000-3428.0064805.

WU Fengyuan, born in 1998, postgraduate. His main research interests include cyberspace security and deep learning.



LIU Shengli, born in 1973, Ph.D professor. His main research interests include network device security and network attack detection.

(责任编辑:喻藜)